PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, G06F 1/00

A1

(11) International Publication Number: **WO 00/30319**

(43) International Publication Date: 25 May 2000 (25.05.00)

(21) International Application Number: PCT/US99/25761

(22) International Filing Date: 5 November 1999 (05.11.99)

(30) Priority Data:
09/191,666 13 November 1998 (13.11.98) US

(71) Applicant: IOMEGA CORPORATION [US/US]; 1821 West Iomega Way, Roy, UT 84067 (US).

(72) Inventors: KUPKA, Michael; 4521 Kenbrook Drive, Nacogdoches, TX 75961 (US). HAWKINS, Michael, L.; 1324 Pruitt Hill Drive #914, Nacogdoches, TX 75961 (US). THOMAS, Trent, M.; 1758 Hillside Circle, Ogden, UT 84403–3214 (US).

(74) Agents: KURTZ, Richard, E. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th floor, One Liberty Place, Philadelphia, PA 19103 (US).

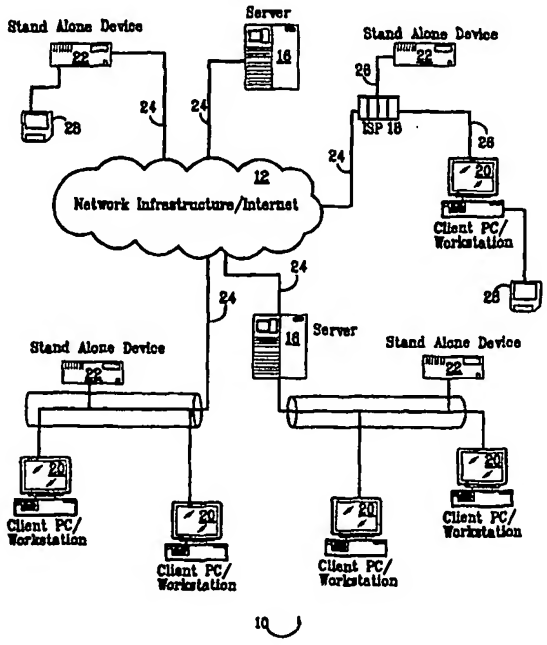
(81) Designated States: CA, CN, JP, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING USING ASYMMETRIC ENCRYPTION AND A UNIQUE IDENTIFIER OF THE MEDIA

(57) Abstract

An apparatus and method of electronically distributing electronic data from a server to a client device via a network infrastructure. The method and apparatus utilizes asymmetric encryption (e.g., public key encryption) to transfer data from a server to a client device. Once the data is received by the client device, it is written to a destination media such that it cannot be accessed from any other piece of media. A unique identifier of the media, which is embedded onto the media during the manufacturing process is used to prevent access from other pieces of media. The downloaded data may also be associated to the media by a compound key that includes the unique identifier of the media, a vendor identifier and a user identifier. The method and system establishes a connection between the client device and the server via the network infrastructure; transmits, via the network infrastructure, the public key; encrypts, at the server, the key to the protected electronic data to be communicated to the client; communicates, via the network infrastructure, the electronic data to the client device, wherein the electronic data is in an encrypted format; decrypts the electronic data in accordance with the key to protected data; and writes, at the client device, the electronic data to the one piece of media, such that the information may be accessed for use from only the one piece of destination media. The electronic data is encrypted and written to the media using either the aforementioned unique identifier or compound key.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM FOR KEYING PROTECTED ELECTRONIC DATA TO PARTICULAR MEDIA TO PREVENT UNAUTHORIZED COPYING USING ASYMMETRIC ENCRYPTION AND A UNIQUE IDENTIFIER OF THE MEDIA

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application is a continuation-in-part of U.S. Patent Application No. 09/061,493, filed April 17, 1998, entitled "System for Keying Protected Electronic Data to Particular Media to Prevent Unauthorized Copying"

FIELD OF THE INVENTION

The present invention relates to the prevention of unauthorized copying by associating electronic data to a particular piece of storage media. In particular, the present invention relates to a remote data delivery system wherein electronic data to be protected is delivered in a secure manner to a local machine which stores and permanently associates the protected electronic data to a particular piece of storage media based on a composite key using at least a unique identifier of the media.

BACKGROUND OF THE INVENTION

Protection of copyrighted and other protected digitally stored data has always been a primary concern of the owners of such material. In particular, piracy of computer

software, music and video has been and continues to be of great concern because it is all but impossible to stop. Although there have been many prior attempts by the software, music, and video industries to curtail piracy, each has been met with limited success.

As part of the effort to combat piracy, software vendors have licensed software rather than transferring ownership when purchased. When software is purchased, the purchaser becomes a licensed user (i.e., licensee) rather than an owner. Copying of software under most license agreements is generally limited to one copy for backup purposes only in order to legally restrict unlimited copying. In addition, the software license typically grants a right to use the software on a single computer or for use by only one user at any time.

Software vendors have also attempted to combat software piracy by copy-protecting their software. While this attempt was effective to some extent, it failed because users were unable to make backup copies. Also, soon after the first copy-protected computer software was on the market, other programs to copy the copy-protected software became available. Other copyright protection methods were then developed in an attempt to stop piracy, also with limited success. These attempts included requiring a master floppy disk to be inserted into the computer or requiring the user to enter a key or other information contained in the user manual or license agreement when executing the software from the computer's hard drive. Still others required a hardware key to be present in the computer's parallel port, which was read when the software was executed. Software vendors received a temporary reprieve when CD-ROMs became the standard media for digital storage and distribution of software, because applications grew to be so large that the only means for copying the software was to "burn" duplicates on expensive recordable CDS. However, the prices of recordable CDS and the drives to write recordable CDS have fallen dramatically and pirates can once again produce cheap illegal copies of protected software.

The music and video industries have a different concern than the software vendors. These industries are particularly concerned with pirates making perfect copies of digitally stored music and videos. While copying of music and video for non-commercial purposes is allowed, such copying has historically been performed by tape decks and video cassette recorders using analog recording techniques. Analog reproduction results in decreasing quality with every generation, whereas digital copies are exact and suffer no

fidelity loss. As noted, prices of recordable CDS and the drives to write to recordable CDS have fallen dramatically and these drives can just as easily record music to the CDS as they record software and data. Further, with the advent of the Digital Versatile Disk (DVD), full length motion pictures may now be recorded to a single DVD disk. As a result, the music and video industries also have a growing need to prevent copying of digitally recorded works.

Fueling the concern of software vendors and the music and video industries is the rapid growth of the digital age and global communications. In the early 1980's when the personal computer (PC) was in its infancy and software vendors first attempted to protect their intellectual property, there were few, if any, mass distribution channels. At the same time period, the music and video industries were strictly analog at the consumer level. Thus, piracy was not a major factor as it was limited to small groups of people or organizations. However, with powerful computers on every desktop and the evolution of music and video into a digital format, piracy has become a major factor costing software vendors alone $4 billion a year worldwide. Clearly, the financial loss to software developers, musicians, actors, and their associated industries is immense.

At the root of the global communications expansion is the rapid growth of the Internet, which has pushed the piracy problem to the forefront. As is well known in the art, the term "Internet" was first used in 1982 to refer to the enormous collection of inter-connected networks that use Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Despite only gaining mass recognition over the past four years, the Internet has existed since the late 1960's and was originally designed as a Wide Area Network (WAN) that would survive a nuclear war. Throughout the 1970's and 1980's a growing number of small networks developed and connected to the Internet via gateways as a means of exchanging electronic mail. In the mid 1980's there was a significant growth in the number of available Internet hosts, and since the late 1980's, the growth of the Internet has been exponential. The growth of the Internet has provided people all over the world with a means to share and distribute information. Thus, the potential now exists for the mass distribution of pirated software, music and video on a global scale. Many Internet Usenet groups and channels on the Internet Relay Chat (IRC) are dedicated to the trading of pirated files, music and videos. Furthering the piracy problem are groups that maintain a high profile and take a great deal of

pride in their piracy accomplishments. The piracy problem has grown so large that a new term, "warez," is used to describe the pirated materials. The Internet now provides a great potential for legitimate sales and distribution of protected software, music and videos, because of its size, speed and penetration into the homes of consumers. However, these very advantages make it easy for pirates to steal expensive, proprietary software that took years to design and manufacture and within hours make it available to anyone, free for the taking.

In view of the above, there is a need for a secure method and apparatus for electronic distribution of data which will take advantage of the wide distribution of networks such as the Internet, while simultaneously preventing unauthorized and illegal copies of protected works, data and applications. In particular, there is a need for a method and apparatus which will provide vendors of software, music and videos with a secure means of electronically distributing their works and applications over the large networks, while ensuring that their protected works and applications are not copied and pirated. Such a method and apparatus would also ensure that the rights of owners of intellectual property are protected and that owners are properly compensated for their creative efforts.

SUMMARY OF THE INVENTION

In view of the above, the present invention, through one or more of its various aspects and/or embodiments is thus presented to accomplish one or more objects and advantages, such as those noted below.

According to an aspect of the invention, there is provided an apparatus and method of electronically distributing electronic data from a server to a client device via a network infrastructure. The method and apparatus utilizes asymmetric encryption (e.g., public key encryption) to transfer data from a server to a client device. Once the data is received by the client device, it is written to a destination media such that it cannot be accessed from any other piece of media. This aspect of the invention is accomplished by using a unique identifier of the media, which is embedded onto the media during the manufacturing process. Alternatively, the downloaded data may be associated to the media by a compound key that includes the unique identifier of the media, a vendor identifier and a user identifier to associate the electronic data with the piece of media. The method and system comprises establishing

a connection between the client device and the server via the network infrastructure; transmitting, via the network infrastructure, the public key; encrypting, at the server, the key to the protected electronic data to be communicated to the client; communicating, via the network infrastructure, the electronic data to the client device, wherein the electronic data is in an encrypted format; decrypting the electronic data in accordance with the key to protected data; and writing, at the client device, the electronic data to the one piece of media, such that the information may be accessed for use from only the one piece of destination media. The electronic data is encrypted and written to the media using either the aforementioned unique identifier or compound key.

Other features of the invention are described below.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary, as well as the following detailed description of the preferred embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there is shown in the drawings an embodiment that is presently preferred, in which like reference numerals represent similar parts throughout the several views of the drawings, it being understood, however, that the invention is not limited to the specific methods and instrumentalities disclosed. In the drawings:

Figure 1 is an exemplary computer network environment in which the present invention may be implemented;

Figure 2 is a block diagram of the components of a client PC/Workstation shown in Figure 1;

Figure 3 is a block diagram of the components of a preferred media drive shown in Figure 2;

Figure 4 is a block diagram of the components of an exemplary stand alone device shown in Figure 1;

Figure 5 is a flow chart illustrating the processes performed in the electronic distribution of data in accordance with the present invention;

Figure 6 is a flow chart illustrating the processes performed in obtaining a unique identifier of the media or building a compound key; and

Figure 7 is an exemplary metafile for use in the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides for a secure method of transmitting sensitive and protected electronic data (protected content) from a remote server to a client computer or stand-alone device over a network infrastructure and for preventing the unauthorized distribution and copying of the data once it is delivered to the client computer or stand-alone device. As used herein, the term "data" includes all information that may be stored on a storage media, including but not limited to, executable files, linked library files, data files, databases files, audio files, and video files.

Referring to Figures 1-4, there is illustrated an exemplary, non-limiting, environment 10 and devices in which the present invention may be implemented. As shown in Figure 1, the environment 10 includes a Wide Area Network (WAN) infrastructure 12. The WAN infrastructure 12 may comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) network such as the Internet. Attached to the WAN infrastructure 12, via communications lines 24, may be one or more Local Area Networks (LAN) 14, servers 16, Internet Service Providers 18, and stand alone devices 22 that are compatible with the protocols of the WAN infrastructure 12. As illustrated, the LAN 14 and ISP 18 may have attached thereto client PC/workstations 20 and/or stand alone devices 22 that may access the network infrastructure 12 via the LAN 14 or ISP 18, and that are capable of at least accessing and reading data on a removable media 28. Also shown is a data decryption/decompressing device 30, which is attached to a PC/workstation 20.

The LAN 14 may comprise an Ethernet or Token Ring network and have a server 16 and gateway (not shown) that provides a connection to the network infrastructure 12 via one or more communications links 24. The communication links 24 to the remote systems may be wireless links, satellite links, or dedicated lines.

The servers 16 may comprise, for example, UNIX-based or Windows NT Server-based computer platform having one or more processors (e.g., Intel Pentium II

processor, Digital Equipment Company Alpha RISC processor, or Sun SPARC Processor), long-term storage (e.g., a RAID disk array), random access memory (RAM), communication peripherals (e.g., network interface card, modem, and/or terminal adapter), and application programs (e.g., database software applications, World Wide Web publishing/hosting software, and inventory management software) which may be used to distribute information to the client PC/workstations 20, stand alone devices 22, and other servers 16. The servers 16 may be configured as, for example, World Wide Web (WWW) servers, File Transfer Protocol (FTP) servers, electronic mail (E-mail) servers, etc. The ISP 18 typically is an organization or service that provides access to the Internet (network infrastructure 12) via a server (not shown) connected to the Internet by communications link 24. In exemplary embodiment of Figure 1, the client PC 20 or stand alone device 22 may utilize a dial-up connection 26 (via the public switched telephone network) to connect to the ISP 18.

The client PCs 20 may comprise Windows 95, Windows 98 or Windows NT Workstation-based personal computers having an Intel Pentium processor or higher, long-term storage (e.g., a IDE or SCSI hard disk), a removable media drive (e.g., CD-R, DVD-RAM, or other removable floppy or hard disk drive), random access memory (RAM), communication peripherals (e.g., network interface card, modem, and/or terminal adapter), and suitable application programs (e.g., Dial-up networking software and a Web Browser). If configured as a workstation, the workstations 20 may comprise, for example, UNIX-based IBM RS/6000 or SUN SPARCStation workstations. Further, the client PC/workstations 20 may comprise the so-called "network computing" devices.

A block diagram of an exemplary PC/Workstation 20 is illustrated in Figure 2. As shown, the PC/Workstation 20 is divided between internal and external components. The internal components include a Basic Input/Output System (BIOS) 70 and a processor (CPU) 66 that control the overall functioning of the PC/Workstation 20. Memory 64, a hard disk drive 76, a floppy disk drive 74, a tape drive 78, a CD-ROM drive 80, a MODEM/Terminal Adaptor/Network Interface Card 82, and a removable media drive 52a are also connected to the CPU 66. The removable media drive 52a or 52b operates to read and/or write to a storage media contained within a removable storage cartridge 28. The exemplary PC/workstation 20 of Figure 2 is configured with two removable media drives 52a and 52b

to emphasize that a removable media drive can be implemented in either internal or external form.

The MODEM/Terminal Adaptor/Network Interface Card 82 may comprise individual cards performing communications-related functions, as known in the art. The MODEM/Terminal Adaptor/Network Interface Cards 82 are included within PC/workstation 20 to provide communications to external networks to which the PC/workstation 20 is connected. In particular, the MODEM/Terminal Adaptor/Network Interface Card 82 may be used to access LAN 14, ISP 18 and network infrastructure 12.

Communications between internal and external devices may be accomplished via controllers provided within the PC/workstation 20. A serial/parallel/USB port controller (which may comprise separate controllers) 58, a monitor controller (video card) 60, and a keyboard and mouse controller 62 each provide an interface between the CPU 66 and an external removable media drive 52b (or printer), monitor 54, and keyboard and mouse device 56, respectively. A hard disk and floppy disk controller 72 serves as an interface between the CPU 66 and the hard disk 76 and the CD-ROM drive 80, and the floppy disk 74 and tape drive 78, respectively. It will be appreciated by those skilled in the art that the disk controller 72 may comprise separate floppy and hard disk controllers (e.g., IDE or SCSI controller).

A removable media controller 68 serves as an interface between the removable media drive 52a and the CPU 66. For example, the removable disk controller 68 may comprise a Small Computer System Interface (SCSI) or Integrated Drive Electronics (IDE) interface controller. A hard disk and floppy disk controller 72 serves as an interface between the CPU 66 and the hard disk 76 and the CD-ROM drive 80, and the floppy disk 74 and tape drive 78, respectively. Alternatively, the removable media drive 52a may utilize the disk controller 72 as an interface to the CPU 66.

Referring now to Figure 3, there is illustrated a block diagram of an exemplary media drive 52 having a SCSI interface to the PC/workstation 20 (via controller 68). The media drive 52 preferably comprises, a ZIP® drive, manufactured by Iomega Corporation, Roy, Utah; however, other media drives may be used as media drive 52. The media drive 52 includes components that provide for communication between the read/write channel for the media (lower right side of diagram) and the PC/workstation 20 (upper left side of diagram).

The media drive 52 includes an AIC chip 101 which performs the SCSI 102, the direct memory access (DMA) 103, and disk formatter 104 functions. The interface also includes a PHAEDRUS 105 which includes an 8032 microcontroller 106, a 1 kByte RAM 107 and an application specific integrated circuit (ASIC) 108. The ASIC 108 may perform various functions, such as servo sequencing, data splitting, EOC, ENDEC, A-to-D, and D-to-A conversion. The communication between the media drive 52 and the PC/workstation 20 is accomplished through transfers of data between the input/output channel of the media drive 52 and the media controller 68 (e.g., SCSI controller) of the PC/workstation 20.

Referring again to Figure 1, the stand alone devices 22, as used herein, may encompass any device capable of interacting with the network infrastructure 12, other than the "traditional" computing device (i.e., PCS, workstations, network computers, or terminals). For example, the stand alone device 22 may include devices such as WebTV®, available from WebTV Networks, Palo Alto, California, a music or video player, etc. It is noted that the stand alone device need not be provided with a communications connection to the network infrastructure, LAN, or ISP.

A block diagram of an exemplary stand alone device 22 is illustrated in Figure 4. The exemplary stand alone device 22 includes a removable media drive 52a, a removable media controller 68, a CPU 66, an ASIC/controller 36, a digital to analog converter 38, ROM 37, and RAM 39. As can be appreciated by one of skill in the art, the stand alone device 22 of Figure 4 may operate as a "player" or "viewer" of the protected data by reading the protected data from the media 28. The removable media drive 52a, the removable media controller 68, and CPU 66 each operate as described in the PC/Workstation 20 of Figures 1-3. ROM 37 contains instructions to control the operation and functions of the stand alone device 22. The ASIC/controller 36 may be used decrypt the protected data and output digital audio and/or video signals (e.g., Pulse Code Modulation (PCM)) to the digital to analog converter 38 for conversion to analog audio or video signals.

Referring again to Figure 1, there is illustrated a decryption/decompressing device 30 in accordance with the present invention, which is connected to the PC 20 to perform the reading/playback/execution of the protected electronic data. The decryption/decompressing device 30 differs from the stand alone device 22 in that the

decryption/decompressing device 30 is not provide with a device (e.g., removable media drive 52) to read the media 28, but rather receives data which is read by, and communicated from, the PC/workstation 20.

It is noted that the exemplary environment and devices shown in Figures 1-4 are not limited to the illustrated environment, as other network infrastructures, communications connectivities, and devices are intended to be within the scope and spirit of the present invention.

Referring now to Figure 5, there is shown the processes performed in accordance with the electronic distribution model of the present invention. As will become evident to those of skill in the art, the features and aspects of the present invention may be implemented by any suitable combination of hardware, software and/or firmware. In accordance with the present invention, the network server or servers 16 may store data, such as application software, database tables, music, video, etc. for distribution to clients 20 and/or stand-alone devices 22. The present invention, while applicable to all types of data transfer, is especially applicable to commerce over the Internet, and in particular, to electronic distribution and delivery of software, music and video data.

The present invention utilizes a public-key, or asymmetric, encryption scheme to encrypt the downloaded data from the sever 16 to the client device 20 (or 22). According to asymmetric encryption, a pair of keys are used in the encryption/decryption process: a public key, which can be given to anyone to encrypt data, and a private key, which is known only to the person desiring to decrypt the data. In contrast to symmetric encryption, the key for decrypting a message is always different from the one used to encrypt it. A more detailed explanation of public-key encryption may be found in Applied Cryptography : Protocols, Algorithms, and Source Code in C, by Bruce Schneier, 2nd edition (December 1995), John Wiley & Sons, which is incorporated herein by reference in its entirety.

An advantage of asymmetric encryption is that the unbreakability of the encryption scheme is based on the length of the keys (i.e., the number of bits). Since modern computers make it possible to use very long keys, it is possible to use keys so long that it would take thousands of years or longer to break them. A disadvantage of asymmetric keys is that symmetric algorithms (where the encryption/decryption keys are the same) are 1000

times faster than public key systems, therefore, it is not practical to use asymmetric systems in real-time on large blocks of data. As will be discussed below, the present invention takes advantage of the strengths of both encryption schemes to prevent unauthorized copying of downloaded data (protected content) once the data has been delivered to a destination media.

In accordance with the present invention, the data key to the encrypted electronic data to be protected is encrypted during the download process using public key encryption, and the data is downloaded and encrypted to the media 28 using a unique identifier (e.g., serial number) of the media 28 as an encryption key. In an alternative embodiment, the data encrypted to the media 28 using a compound key as an encryption key that comprises the unique identifier of the media 28, a vendor identifier and a user identifier. In order to ensure that each particular piece of media 28 has a unique identifier, the unique identifier is permanently embedded on the media 28 during the manufacturing process and is not accessible by a user or a disk drive that reads/writes to the media 28 at a later time. Further, a user format of the media 28 will not erase or alter the embedded serial number. Thus, the downloaded encrypted protected electronic data is then associated to the media 28 by the unique identifier and may not be accessed from any other media having a different or no unique identifier. Further, if the compound key is used to write the data to the media 28, the protected electronic data may not be accessed from any other media and also may not be accessed if the vendor or user identifiers are incorrect.

Referring again to Figure 5, at step 200 the process begins after a user on the client PC 20 (stand alone device 22) has contacted and connected to a server 16 (Web server) via, e.g., a Web browser, and makes a selection of protected data for downloading. The user initiates the electronic data distribution process when he or she desires to purchase software, music or videos (i.e., protected electronic data) using a home personal computer 20 or stand alone device 22 (client device). The protected electronic data may be offered for sale for a fee from e.g., a World Wide Web (WWW) site residing on one of servers 16, and purchased using a credit card, debit card, smart card, virtual cash, etc. To this end, the home user may connect, via an Internet browser such as Internet Explorer available from Microsoft, Redmond, WA, to the WWW site by entering the universal resource locator (URL) or "clicking" a hyper-text link that contains the WWW site's URL. The URL may contain, e.g., an Internet Protocol

(IP) address (e.g.,147.178.20.151) or a domain name (e.g., "sitename.com") that identifies the IP address of the site such that the browser may establish a TCP/IP connection. It is preferable, that the Web sever 16 comprises an Iomega store web server 16, which will be described below. It is preferable that the connection to the Web server is a secure (i.e., encrypted) connection. After the user clicks on the download button of the displayed web page from the Web server, this action causes the PC/workstation to submit an HTML form to the web server 16. The web server 16 then executes the appropriate Common Gateway Interface (CGI) program. The CGI program running on the Iomega store web server 16 sends the metatag "Content-Type: application/x-itf" followed by an appropriate Iomega Transaction File (ITF) to the client PC/workstation 20. The ITF file is unique to the Iomega store web server 16 and is used to provide information to an ITF client program which controls the download process at the client side. The format of the ITF file is shown in Figure 7. As the web browser receives the metatag, it launches the ITF client program and passes the ITF file name as a command line parameter. The ITF client application opens the ITF file and parses the metadata from the metatags. The client PC/workstation 20 will connect to the server address provide by the ITFSERVER tag to receive the electronic data. The server address may be dynamically changed for each request in order to balance the load on the server. For example, the ITF file may include the following information for a transfer of a single file containing a song:

<ITFVERSION:>0.1
<ITFNEWFILE:>
<ITFID:>2
<ITFSERVER:>147.178.20.151
<ITFFILENAME:>D:\WebSite\htdocs\html\ZipMan\Samples\SuppReady.mp3
<ITFARTIST:>Genesis
<ITFTITLE:>Supper's Ready
<ITFALBUM:>Foxtrot
<ITFCOST:>$2.50
<ITFDATE:>3/4/98
<ITFSIZE:>4746500

At step 202 the client system 20 (or 22) generates two keys, a public key (K1), and a private key (K2). The keys have a predetermined size and may be generated using ANSI Standard X9.17 or using a sequence of digits taken for a real-time clock running in hardware on the client device (a pseudo-random number generator).

At step 204 the client system 20 connects to the server 16 identified in the ITFSERVER tag (e.g., 147.178.20.151), and sends a command packet to the server via TCP/IP sockets. The first command packet has an action code of one and contains the file name to be transferred, all the customer information, billing information, and the public key (K1). The first command packet may be formatted as follows:

```
struct SocketCommand
{
  unsigned long  Code;
  unsigned long Size;
  unsigned char Data[400];
};
```

Alternatively, the Data field may comprise a plurality of fields containing the customer information, billing information, and the public key (K1) as parsed fields. The data field may be formatted to have the following data structure:

```
{
  char First[20];
  char Last[20];
  char Address[40];
  char City[20];
  char State[3];
  char Zip[6];
  char CreditCard[17];
  char ExpDate[5];
  char Phone[13];
  char Key[128];
  long int DataID;
};
```

At step 206 the server 16 uses the client's public key (K1) to encrypt the Copy Protected Data Key (K3). The copy protected data key (K3) is a key used to encrypt/decrypt the data stored on the server 16. At step 208, the server 16 responds with a data packet with the same action code and informs the client 20 that the file has been opened and the file size. In addition, the server 16 transmits the encrypted copy protected data key (K3) to the client 20. At step 210, the client device 20 decrypts the encrypted copy protected data key (K3) using the client's private key (K2). The copy protected data key (K3) may then be stored in RAM 64 for subsequent use to decrypt the copy protected data as it is received by the client device 20.

At step 211, the client device 20 (or 22) sends a command packet with an action code of two, which informs the server to send the next 4000 bytes of pre-encrypted data. It is noted that this action code is repeated until the entire file has been transferred from the server 16 to the client PC 20 or stand alone device 22 (via the process of steps 211 through 218, as described below). At step 212 the server 16 server transmits the pre-encrypted copy

protected data to the client device 20 via, e.g., TCP/IP sockets. The data transmitted to the client PC 20 from the server 16 is preferably in a predetermined data structure such as the following:

```
struct SocketData
{
  unsigned int  Code;
  unsigned long FileSize;
  unsigned char Data[4000];
};
```

At step 214, the client decrypts the copy-protected data using the copy protected data key (K3). Alternatively, at steps 212 and 214, the system may provide for double encryption by encrypting the pre-encrypted copy protected data a second time for transmission to the client device 20 using the public key (K1) and decrypted using the private key (K2) and then the copy protected data key (K3). Upon completion of step 214, the data is in decrypted state and ready to be written to the media 28 such that it is permanently associated to the media 28 in accordance with the present invention.

The association of the data to the media 28 begins at step 216 where the ITF client program encrypts obtains the unique identifier of the media 28 (first embodiment) or the compound key (second embodiment), which will be used to associate the data to the media 28. Referring now to Figure 6, at step 300, the ITF client program determines if it is the first time that a portion of the protected data will be written to the media 28. If so, the client PC 20 queries the particular piece of media 28 to which the downloaded content is to be stored for the media's unique serial number. By way of a non-limiting example, the media 28 may comprise a ZIP® disk manufactured by Iomega Corporation, Roy, Utah. Each Iomega ZIP® disk contains a unique serial number that is written to a predetermined track during the formatting process which may be used as the unique identifier. The serial number is preferably created by but not limited to a pseudo random number generator. Further, while the media 28 has been described in terms of a ZIP® disk, it is not limited to the ZIP® disk, as the use of other removable and permanent media types having a unique identifier is within the

scope and spirit of the present invention such as CD-R, DVD-RAM, and other removable floppy and hard disks.

The client PC 20 may query the media using an application programming interface (API) such as the Iomega Ready API, or other suitable method. The Iomega Ready API when invoked causes the media drive to read the unique serial number from the predetermined track by using the SCSI 0x06 Non-Sense Command. In particular, by invoking the Disk Status Page (page 0x02) of the Non-Sense Command, the media serial number may be determined by reading offset bytes 20-59 of the returned data structure. Exemplary source code for performing step 302 in conjunction with an Iomega ZIP® drive and disk is as follows:

```
void CClientApp::GetZipDrive()
{
        int j,k;
        m_DriveNum = 0;
        for(j = 0;j < 26;j++)
                // scan the drives and find the IOMEGA drives
        {
                if(IsIomegaDrive(j) )
                {
                        k = GetGeneralDevType(j);
                        if( k == DRIVE_IS_ZIP )
                        {
                                m_DriveNum = j;
                                j = 26;
                        }
                }
        }
}

void CClientApp::GetSerialNumber()
```

```
{
        unsigned char szBuffer[1024];
        memset(szBuffer,0,sizeof(szBuffer));
        memset(&m_SerialNumber,0,40);
        GetInfoNonSense(m_DriveNum,0x02,szBuffer);
        memcpy(&m_SerialNumber,&szBuffer[22],39);
}
```

It can be appreciated that the unique identifier is not limited to information stored on the media 28 such as the serial number, and that other types of information could be used as the unique identifier, so long as it is permanently stored on the media 28. In addition, the unique serial number should contain a sufficient number of bits (length) to ensure that no two pieces of media have the same identifier. For example, each Iomega ZIP® disk contains a unique 39 byte (312 bits) serial number, and other bit lengths may be utilized. After obtaining the unique identifier it is stored in RAM 64 for subsequent use. If operating under the first embodiment (i.e., writing the data to media 28 in accordance with the unique identifier only) then the process returns at step 312 to step 217 (Figure 5).

However, in accordance with a second embodiment additional security is provided for by including not only the unique identifier in the encryption/decryption key, but also a vendor identifier and a user identifier. Such an encryption/decryption key will be referred to herein as a compound key. In particular, by using the compound key having vendor information and user information, certain additional safeguards may be built into the distribution of the protected data. The vendor information may be an identifier created by the vendor of the protected content or an industry group. The purpose of this identifier is to allow the vendor or an industry group to add additional layers of security to prevent unauthorized decryption of protected data by a person or software program not approved by the vendor or industry group. For example, as will be discussed below, the vendor information may be retrieved from application software downloading, running or playing the protected content, thus further restricting use of the content to devices having licenced copies of the application

software. Alternatively, the vendor information may retrieved from a server located on a local area network (LAN), wide area network (WAN), or the Internet, etc.

The user information is information that is specific to an individual user or group of users. This identifier may be created by the user or on the user's behalf by the software application. The user identification provides for user control over access to the protected content. Such user control may be desirable in corporate environments to allow only authorized users (e.g., company officers, specific departments and specific individuals) access the protected content. In the home, user control will provide parents with a mechanism by which to prevent children from accessing inappropriate content (e.g., R-rated movies).

In accordance with the second embodiment, at step 304, the vendor information is obtained. Such information may be embedded by known means within the ITF client program which controls the download process at the client side. As such, each vendor would have a unique ITF client program to perform the download process. Alternatively, a generic ITF client program may be executed at the client side and the vendor information retrieved from a file on the client PC 20, stand alone device 22, or from a database on the server 16 that associates the protected content to the vendor information via known processes.

At step 306, the user information is obtained. This is preferably performed by prompting the user for the information. The user then enters the information, which is temporarily stored in RAM 64 or on the hard disk 76. Alternatively, a separate software application may be invoked to provide the user information (e.g., a password application that retrieves a user's password from a network yellow pages file).

At step 308, the compound encryption/decryption key is built and stored in RAM 64. The process may be performed by combining the three key components (e.g., the unique identifier of the media 28, the vendor information, and the user information) by any means, including but not limited to, mathematical operations (mod, addition, division, subtraction, XOR, etc.) concatenation, interleaving, or any other method. Preferably, byte level interleaving of the vendor information and the user information is performed. This results in a string having the structure: V0U0V1U1V2U2V3U3V4U4V5U5V6U6V7U7, where Vx is vendor information byte x, and Ux is user information byte x. The resulting

string is then combined with the unique serial number by an XOR (exclusive OR) operation to form the compound key. Thus, the compound key is preferably created as follows:

CK = S XOR (V interleaved U)

wherein,

CK= Compound Key

S= Serial Number

V= Vendor Information

U= User Information

The process then proceeds to step 312, where it returns to step 217 (Figure 5).

If at step 300 it is determined by the ITF client application that a portion of the downloaded data has been written to the media, the unique identifier or compound key will have already been obtained in either steps 302 (first embodiment) or 308 (second embodiment) and stored in RAM 64. As such, at step 310, the ITF client application retrieves the unique identifier or compound key from RAM 64 and returns at step 312 to step 217 (Figure 5).

It is noted that the unique identifier and compound key have been described as being obtained then stored in RAM. This advantageously speeds the download process. However, to insure that the media 28 is not removed during the download process, the unique identifier or compound key may be obtained at each write (by re-executing steps 302 and 304-308) to the media 28. It is noted that this second method may be slower than the above due to the increased disk access activity.

Referring again to Figure 5, at step 217, the client device 20 encrypts downloaded content using the unique serial number (first embodiment) or compound key (second embodiment) as an encryption key. While any suitable encryption algorithm may be utilized at step 217, the data encryption is preferably performed using the well known Blowfish encryption algorithm. The Blowfish encryption algorithm is advantageously fast, especially when implemented on 32-bit microprocessors with large data caches, such as the

Intel Pentium and the IBM/Motorola PowerPC. Briefly, Blowfish is a variable-length key, 64-bit block cipher which may be implemented in either hardware or software. The algorithm consists of two parts: a key-expansion part and a data-encryption part. The key expansion part converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network, wherein each round consists of a key-dependent permutation and a key- and data-dependent substitution. All operations are exclusive ORs (XOR) and additions on 32-bit words. The only additional operations are four indexed array data lookups per round to generate the encrypted data.

At step 218, the client device writes the encrypted copy protected data to the media 28. The data may be written to the media 28 in a standard file system structure or by direct track or sector writes. The format by which the data is written to the media 28 is not limited to the noted formats, as other formats may be utilized.

The process of step 211-218 repeats until all of the data has been downloaded from the server 16 to the client PC 20. At that time the client PC 20 will send an action code of three to inform the server 16 that the transaction is complete and to disconnect the socket (step 220). It is noted that the source code and data structures above are included herein for exemplary purposes only, and are in no way intended to limit the scope of the present invention.

As noted above, the data is stored on the media 28 in an encrypted format using at least the unique serial number as a decryption key. The encryption/decryption key may also be a compound key that includes the unique serial number of the media, vendor information and user information. Accordingly, if the data is copied to any other media, the decryption process will fail rendering the content unusable. Thus, unauthorized copying of data downloaded using the apparatus and method of the present invention will be prevented. Further, while process described above refers to a client PC, the process is applicable to a stand alone device capable of communicating over the network infrastructure, and reading and writing to the media on which the protected electronic data is stored. For example, a kiosk may be provided at retail outlets where purchasers may insert a piece of media 28 into the kiosk and download data to be used on a home or office personal computer.

In accordance with the present invention, the server 16 may store digital content to be downloaded in an encrypted or unencrypted format. If the digital content to be downloaded is not stored in an encrypted format, then it is preferably encrypted upon downloading using a public key as an encryption key. Also, as noted above, if the digital content to be download is stored on the server 16 in an encrypted format (pre-encrypted) prior to downloading then the server may encrypt the data key (e.g., copy protected data key K3) to the content (i.e., the software application, music or video) or the content itself (double encryption). Pre-encryption may be preferable to provide greater performance in environments where large amounts of data need to be encrypted per transaction. Such electronic distribution systems may be heavily burdened if they were required to encrypt the entire content that is to be electronically distributed.

Once the downloaded content has been written to the media 28, it will likely be played/executed/run by a user numerous times. Exemplary players and devices to execute or use the downloaded data may be found in U.S. Patent Application No. 09/061,493, filed April 17, 1998, entitled "System for Keying Protected Electronic Data to Particular Media to Prevent Unauthorized Copying" and Attorney's Docket Number IOM-2793, filed November 13, 1998.

It is noted that the foregoing examples have been provided merely for the purpose of explanation and are in no way to be construed as limiting of the present invention. While the invention has been described with reference to preferred embodiments, it is understood that the words which have been used herein are words of description and illustration, rather than words of limitations. Further, although the invention has been described herein with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed herein; rather, the invention extends to all functionally equivalent structures, methods and uses, such as are within the scope of the appended claims. Those skilled in the art, having the benefit of the teachings of this specification, may effect numerous modifications thereto and changes may be made without departing from the scope and spirit of the invention in its aspects.

For example, fixed media having a unique identifier may be utilized by the present invention to receive protected electronic data. Also, the removable media need not

be a removable media cartridge, but may comprise a removable drive, such as those which are removably connected to personal computers or other devices via, e.g., drive bays, device bays, and PCMCIA slots.

WHAT IS CLAIMED IS:

1. Canceled

2. A method of electronically distributing electronic data from a server to a client device via a network infrastructure, said method utilizing asymmetric encryption and a unique identifier of a piece of media to which the electronic data is downloaded to associate the electronic data with only said piece of media, said method comprising:

establishing a connection between the client device and the server via the network infrastructure;

generating first and second data encryption keys, said first and second data encryption keys being asymmetric keys;

transmitting said first key to the server;

encrypting at least one of a protected data key to the electronic data and the electronic data at the server in accordance with said first data key;

communicating the electronic data to the client device;

decrypting at least one of said protected data key to the electronic data and the electronic data at the client device in accordance with said second data key;

encrypting the electronic data at the client device using said unique identifier; and

writing the electronic data to said piece of media, such that the electronic data may be accessed for use from only said piece of destination media.

3. The method as recited in claim 2, further comprising:

accessing one piece of destination media; and

reading said unique identifier from a predetermined location on said piece of destination media.

4. The method as recited in claim 3, further comprising:

obtaining a vendor identifier; and

obtaining a user identifier,

wherein said step of encrypting the electronic data at the client device using said unique identifier further comprises building a compound key through a predetermined operation using said unique identifier, said vendor identifier, and said user identifier, and encrypting the electronic data using said compound key.

5. The method as recited in claim 3, wherein said predetermined location on said piece of destination media is a predetermined track.

6. The method as recited in claim 2, wherein said encrypting of the electronic data to be transmitted to the client device comprises encrypting said protected data key to the electronic data and the electronic data.

7. The method as recited in claim 2, wherein said establishing a connection between the client device and the server via the network infrastructure comprises:

submitting, from the client device, a form to the server;

executing, at the server, a program to process said form; and

sending, to the client, a metatag and transaction file.

8. The method as recited in claim 7, wherein said metatag and said transaction file launch a client program at the client device after being sent to the client device.

9. The method as recited in claim 8, wherein said client program opens said transaction file and parses metadata from metatags within said transaction file, and wherein the client connects to a server address identified by a predetermined metatag in said transaction file to receive the electronic data.

10. The method as recited in claim 9, wherein said server address is dynamically changed as the electronic data is requested from the server.

11. The method as recited in claim 2, said communicating the electronic data to the client device comprising communicating said protected data key to the client device.

12. An apparatus for communicating electronic data over a network infrastructure, said apparatus utilizing asymmetric encryption and a unique identifier of a piece of media to which the electronic data is downloaded to associate the electronic data with only said piece of media, said apparatus comprising:

a communications interface to the network infrastructure;

a processor which controls and executes instructions to receive the electronic data and to access said piece of media to obtain said unique identifier; and

a media drive, responsive to said processor, which reads said unique identifier from said piece of media inserted therein,

wherein said apparatus establishes a connection with a server over the network infrastructure and communicates a first data key to the server,

wherein the server encrypts at least one of a protected data key to the electronic data and the electronic data in accordance with said first data key and communicates the electronic data to said apparatus, wherein said apparatus decrypts at least one of said protected data key to the electronic data and the electronic data in accordance with said second data key, and

wherein said apparatus encrypts the electronic data using said unique identifier and writes the electronic data to said piece of media, such that the electronic data may be accessed for use from only said piece of destination media.

13. The apparatus as recited in claim 12, wherein said apparatus reads said unique identifier from a predetermined location on said piece of destination media.

14. The apparatus as recited in claim 13, wherein said apparatus further obtains a vender identifier and a user identifier, wherein encrypting the electronic data is performed using a compound key that is created through a predetermined operation using said unique identifier, said vendor identifier, and said user identifier.

15. The apparatus as recited in claim 12, wherein the server encrypts said protected data key to the electronic data and the electronic data before communicating the electronic data to said apparatus.

16. The apparatus as recited in claim 12, wherein said apparatus communicates a form to the server, wherein the server process said form, and wherein apparatus receives a metatag and transaction file.

17. The apparatus as recited in claim 16, wherein said metatag and said transaction file launch a client program at said apparatus.

18. The apparatus as recited in claim 17, wherein said client program opens said transaction file and parses metadata from metatags within said transaction file, and wherein said apparatus connects to a server address identified by a predetermined metatag in said transaction file to receive the electronic data.

19. The apparatus as recited in claim 18, wherein said server address is dynamically changed as the electronic data is requested from the server.

20. An apparatus for communicating electronic data over a network infrastructure in accordance with public key encryption, said apparatus further associating the electronic data to a piece of media to which the electronic data is downloaded in accordance with a compound key, said apparatus comprising:

a communications interface to the network infrastructure;

a processor which controls and executes instructions to receive the electronic data and to access said piece of media to obtain said unique identifier; and

a media drive, responsive to said processor, which reads said unique identifier from said piece of media inserted therein,

wherein said apparatus establishes a connection with a server over the network infrastructure and communicates a public key to the server,

wherein the server encrypts a protected data key to the electronic data in accordance with said public key and communicates the electronic data to said apparatus, wherein said apparatus decrypts said protected data key to the electronic data in accordance with a private key, and

wherein said apparatus encrypts the electronic data using said compound key that is created through a predetermined operation using said unique identifier, a vendor identifier, and a user identifier and writes the electronic data to said piece of media, such that the electronic data may be accessed for use from only said piece of destination media.

21. The apparatus as recited in claim 20, wherein said vendor identifier and said user identifier and said user identifier is obtain by a client program running on said apparatus, and wherein said client program is launched upon receipt of a metatag and transaction file from the server.

22. The apparatus as recited in claim 21, wherein said client program opens said transaction file and parses metadata from metatags within said transaction file, and wherein the client connects to a dynamically assigned server address identified by a predetermined metatag in said transaction file to receive the electronic data.

23. An apparatus for communicating electronic data over a network infrastructure in accordance with public key encryption, said apparatus further associating the electronic data to a piece of media to which the electronic data is downloaded in accordance with a compound key, said apparatus comprising:

a communications interface to the network infrastructure;

a processor which controls and executes instructions to receive the electronic data and to access said piece of media to obtain said unique identifier; and

a media drive, responsive to said processor, which reads said unique identifier from said piece of media inserted therein,

wherein said apparatus establishes a connection with a server over the network infrastructure and communicates a public key to the server,

wherein the server encrypts a protected data key to the electronic data in accordance with said public key and communicates the electronic data to said apparatus, wherein said apparatus writes said protected data key and said electronic data to said one piece of media, and

wherein said apparatus decrypts said protected data key to the electronic data in accordance with a private key residing in said apparatus and decrypts said electronic data in accordance with said data key such that said electronic data may be accessed for use from only said one piece of destination media.

FIG. 1

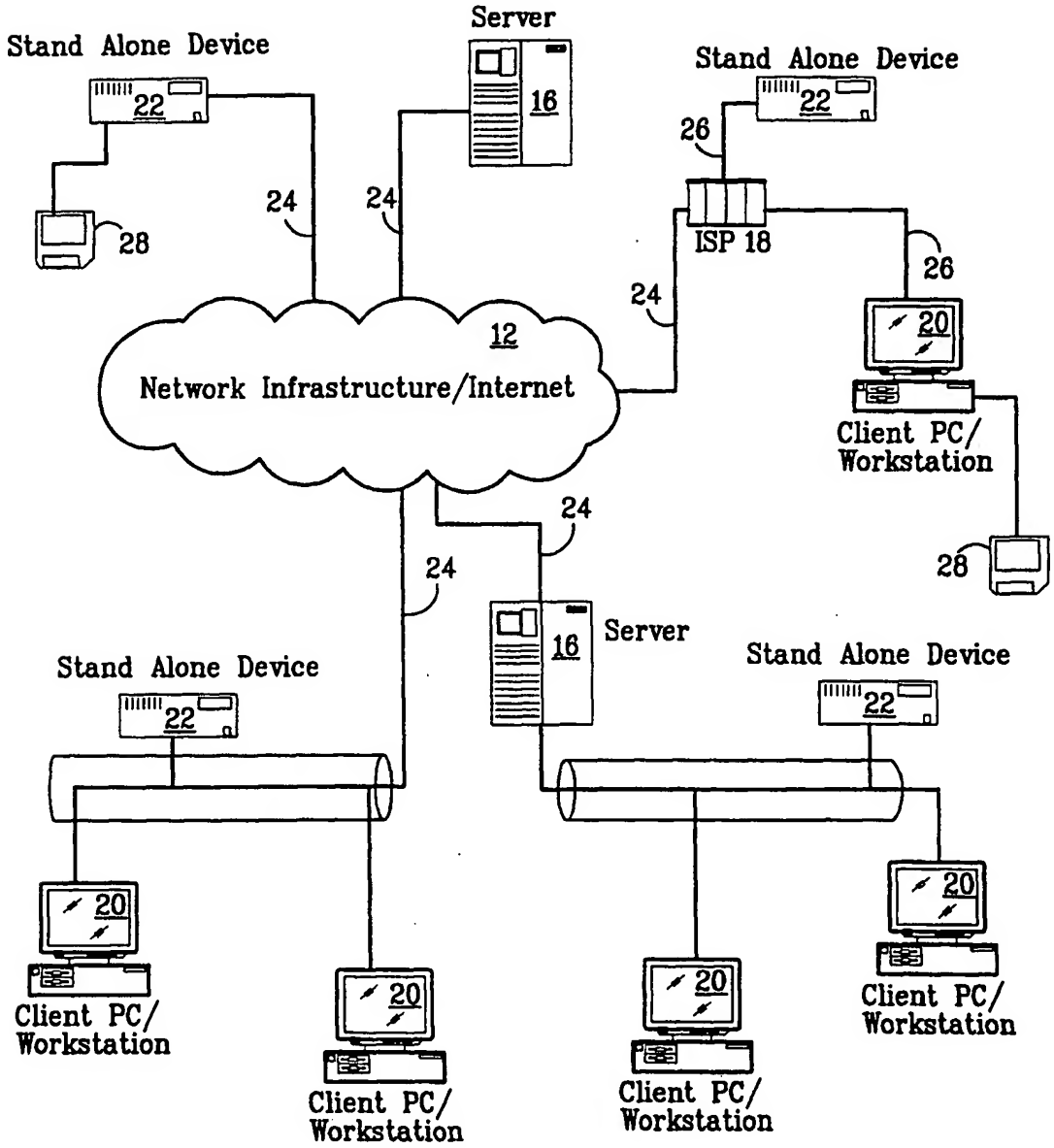
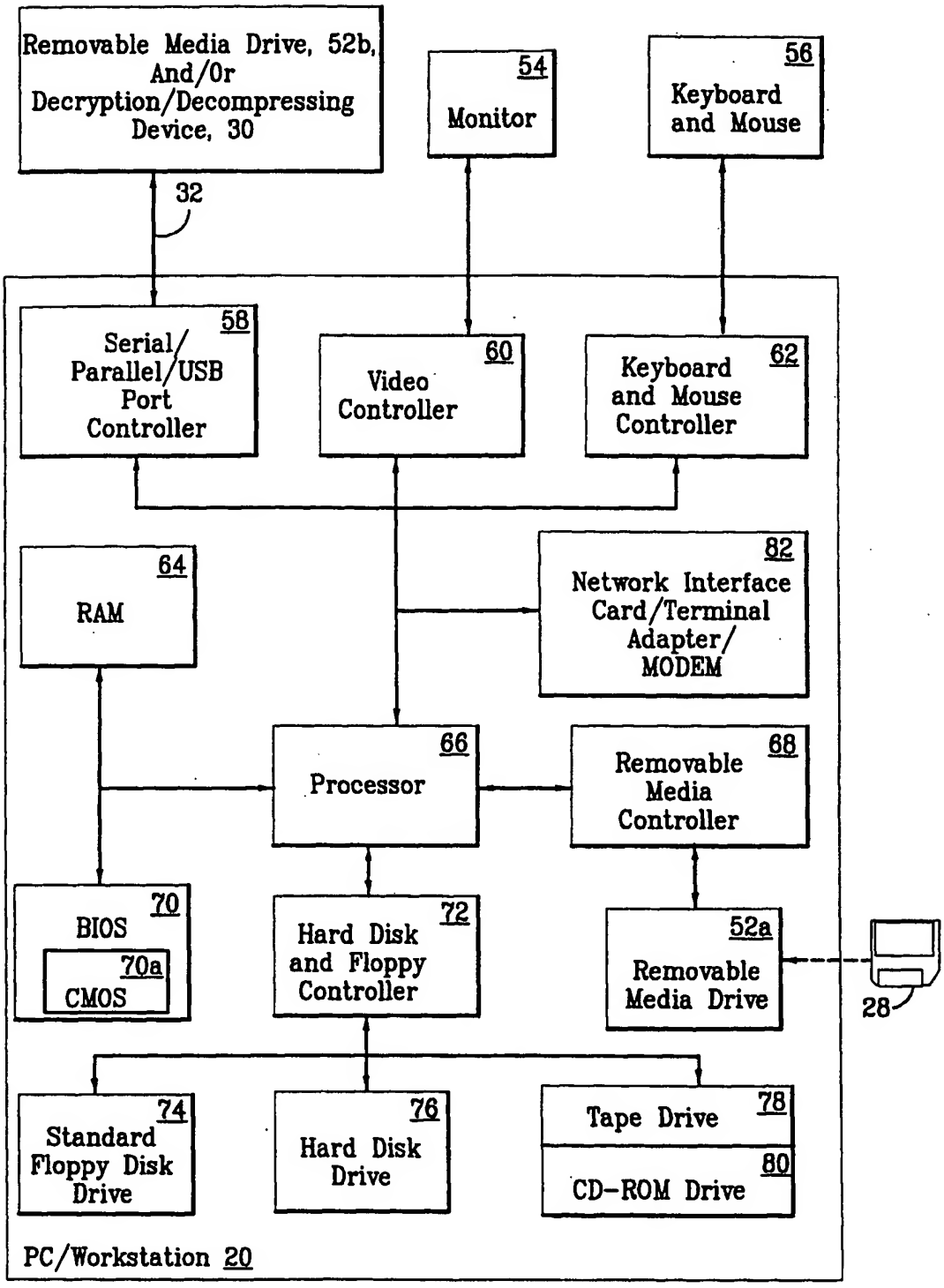

Server
16
Stand Alone Device
22
Stand Alone Device
22
26
ISP 18
26
24
24
24
28
12
Network Infrastructure/Internet
20
Client PC/
Workstation
28
24
24
Server
16
Stand Alone Device
22
Stand Alone Device
22
20
Client PC/
Workstation
20
20
Client PC/
Workstation
20
Client PC/
Workstation
10

FIG. 2


Removable Media Drive, 52b, And/Or Decryption/Decompressing Device, 30
32
54
Monitor
56
Keyboard and Mouse
58
Serial/ Parallel/USB Port Controller
60
Video Controller
62
Keyboard and Mouse Controller
64
RAM
82
Network Interface Card/Terminal Adapter/ MODEM
66
Processor
68
Removable Media Controller
70
BIOS
70a
CMOS
72
Hard Disk and Floppy Controller
52a
Removable Media Drive
28
74
Standard Floppy Disk Drive
76
Hard Disk Drive
78
Tape Drive
80
CD-ROM Drive
PC/Workstation 20

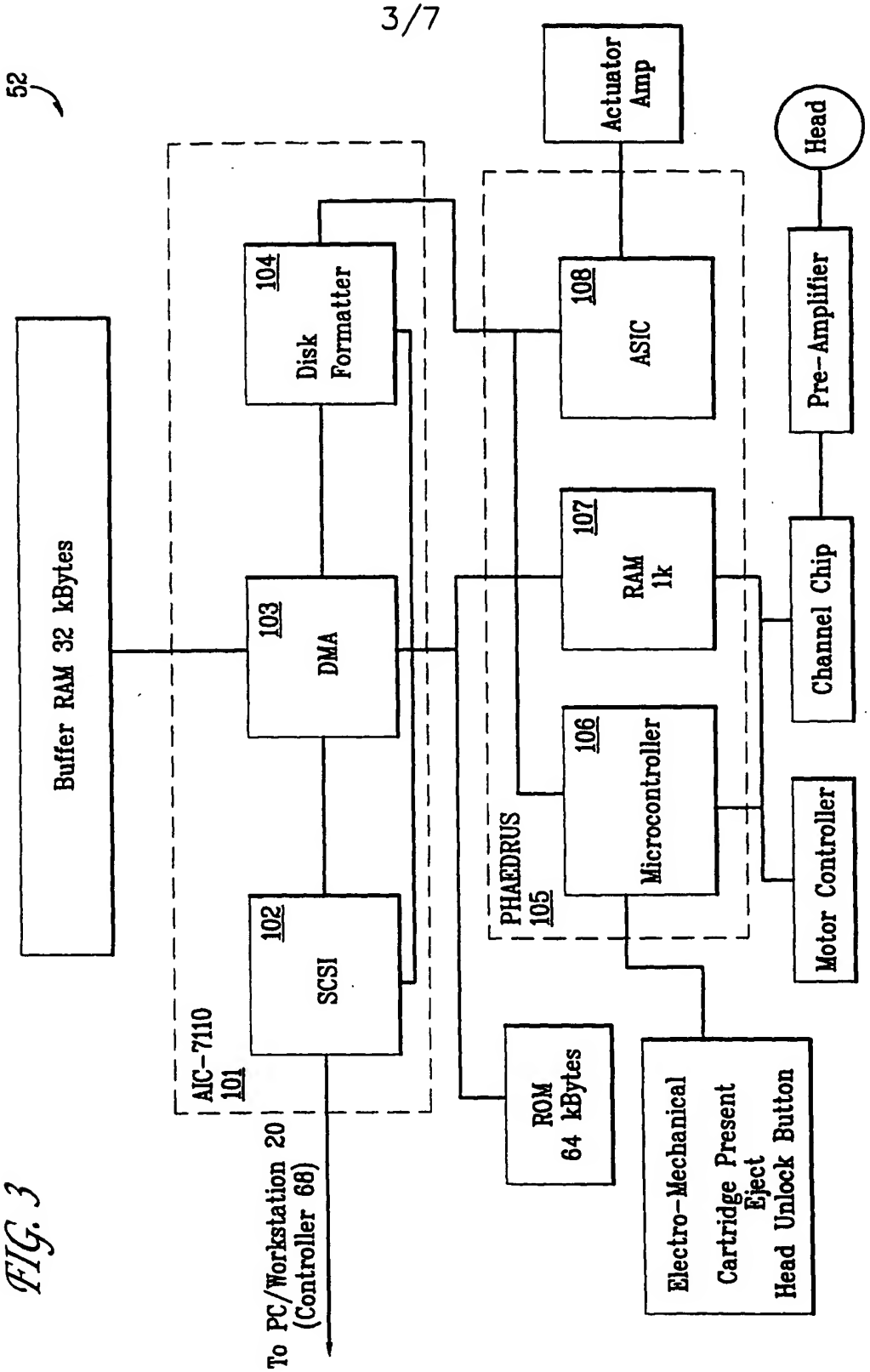

52
Buffer RAM 32 kBytes
AIC-7110
101
104
Disk
Formatter
103
DMA
102
SCSI
To PC/Workstation 20
(Controller 68)
PHAEDRUS
105
108
ASIC
107
RAM
1k
106
Microcontroller
ROM
64 kBytes
Electro-Mechanical
Cartridge Present
Eject
Head Unlock Button
Actuator
Amp
Head
Pre-Amplifier
Channel Chip
Motor Controller

FIG. 3

FIG. 4

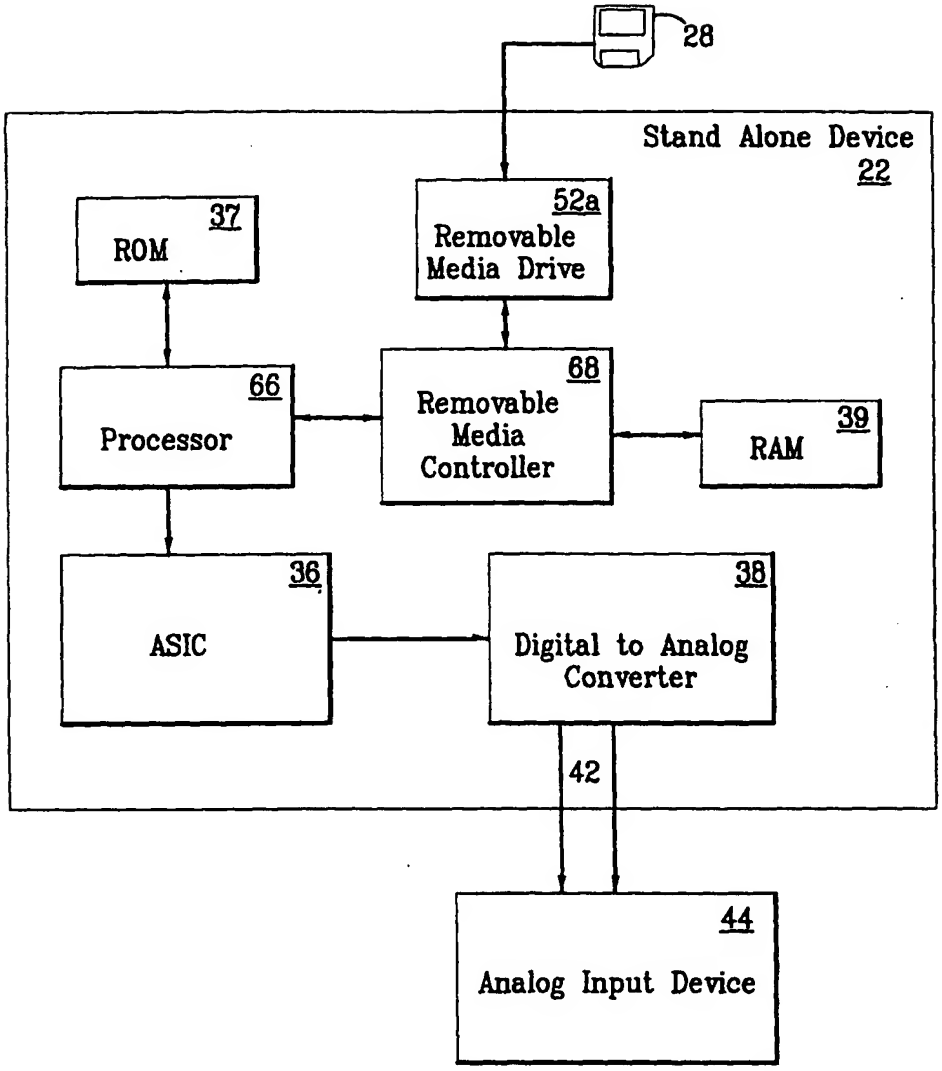
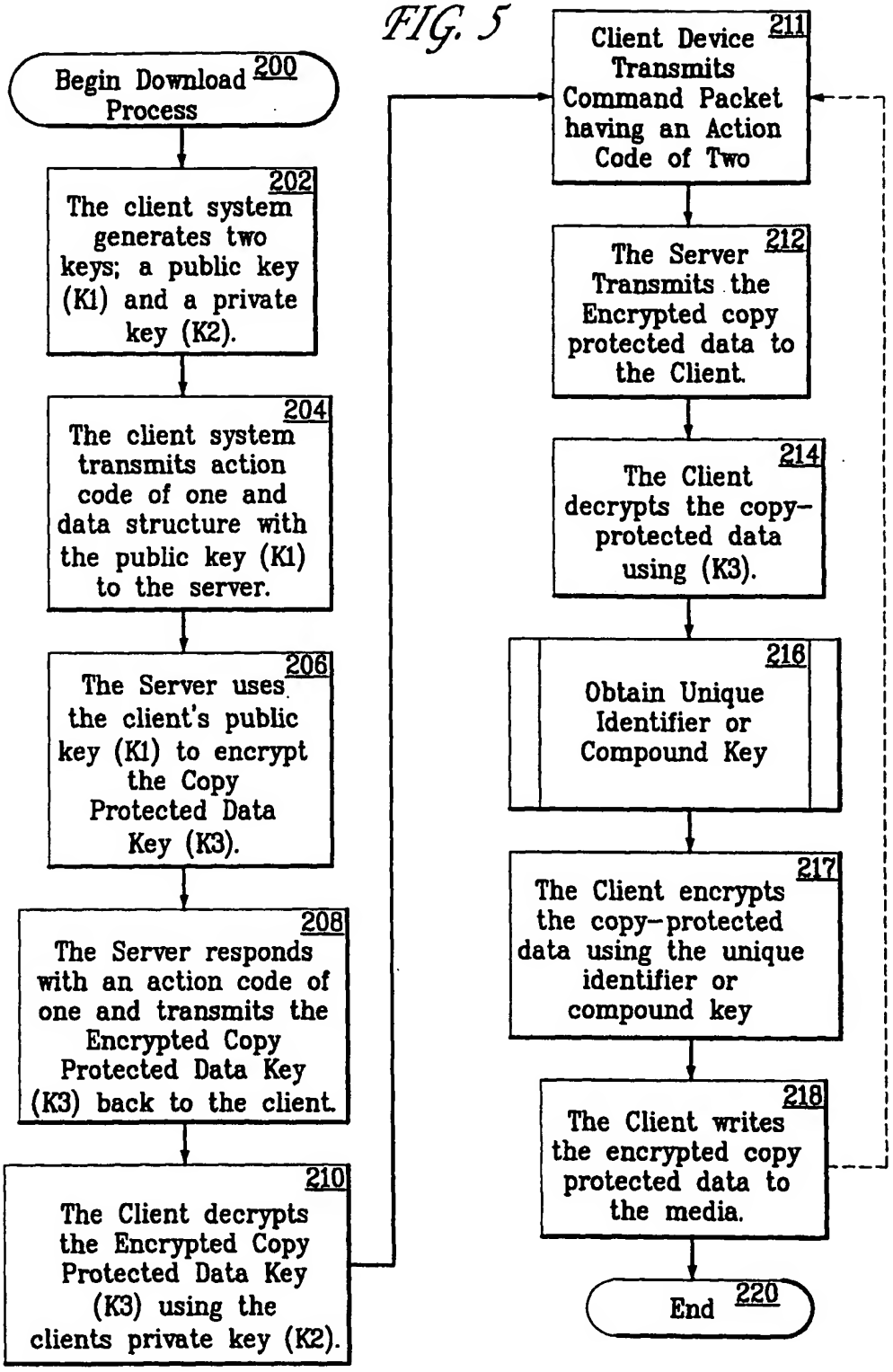

28
Stand Alone Device
22
37
ROM
52a
Removable
Media Drive
66
Processor
68
Removable
Media
Controller
39
RAM
36
ASIC
38
Digital to Analog
Converter
42
44
Analog Input Device

FIG. 5


Begin Download Process 200
202 The client system generates two keys; a public key (K1) and a private key (K2).
204 The client system transmits action code of one and data structure with the public key (K1) to the server.
206 The Server uses the client's public key (K1) to encrypt the Copy Protected Data Key (K3).
208 The Server responds with an action code of one and transmits the Encrypted Copy Protected Data Key (K3) back to the client.
210 The Client decrypts the Encrypted Copy Protected Data Key (K3) using the clients private key (K2).
211 Client Device Transmits Command Packet having an Action Code of Two
212 The Server Transmits the Encrypted copy protected data to the Client.
214 The Client decrypts the copy-protected data using (K3).
216 Obtain Unique Identifier or Compound Key
217 The Client encrypts the copy-protected data using the unique identifier or compound key
218 The Client writes the encrypted copy protected data to the media.
End 220

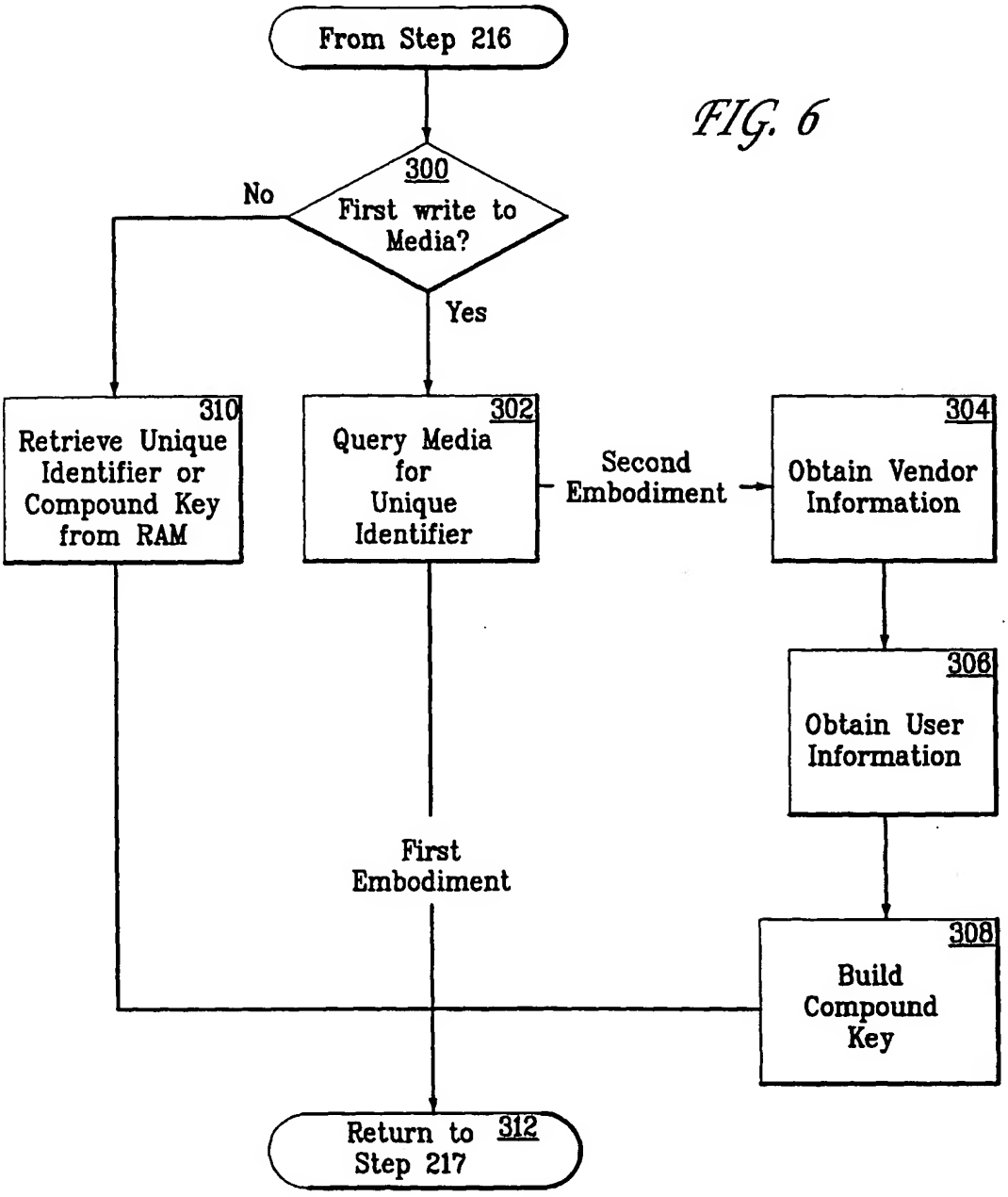

From Step 216
300
First write to Media?
No
Yes
310
Retrieve Unique Identifier or Compound Key from RAM
302
Query Media for Unique Identifier
Second Embodiment
304
Obtain Vendor Information
306
Obtain User Information
First Embodiment
308
Build Compound Key
Return to Step 217
312

FIG. 6

FIG. 7

Meta Tags

1. IPMVERSION: ITF Format Version number specified in n.n major, minor format. Example is <ITFVERSION>: 0.1

2. ITFNEWFILE: This Metatag indicates a new block of Metatags and Metadata follows. Should be the first Metatag following the ITFVERSION Metatag. This Metatag is designed to allow compound ITF Files which may be used for Batch Downloads.

3. ITFFID: This tag holds the database id for this item.

4. ITFSERVER: Specifies the IP link to the server that contains the file to be processed. May be DNS entry or IP number. Prefer IP number so we don't have to rely on DNS translation.

5. ITFFILENAME: The name of the file to be processed.

6. ITFARTIST: The song artist. May be multiple names comma delimited.

7. ITFTITLE: The song title.

8. ITFALBUM: The name of the album the song is from.

9. ITFCOST: This tag contains the item's cost.

10. ITFDATE: Date file was created, or last updated. Mm/dd/yy

11. ITFSIZE: This tag contains the file size of the item.

Usage Rules
1. All Metatags begin with the Less than sign, '<', and end with colon greater than, ':>'.
2. All Metatags must begin in the first column of a line.
3. Metadata immediately follows the closing :> of the Metatag and ends with either a new Metatag or the end of file. This allows the usage of any characters or text sequence including the characters used to delimit the Metatag itself. Caveat, do not attempt to embed a Metatag inside the Metadata if the embedded Metatag begins on a new line.

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/US 99/25761

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 757 908 A (PRYOR ROBERT FRANKLIN ET AL) 26 May 1998 (1998-05-26) column 1, line 38 -column 2, line 65 column 6, line 61 -column 7, line 67 column 14, line 28 - line 40 column 21, line 45 - line 56	2,12,20, 23
A	EP 0 665 486 A (AT & T CORP) 2 August 1995 (1995-08-02) abstract column 1, line 34 -column 2, line 5 column 3, line 6 - line 13 column 6, line 29 -column 8, line 28	2,12,20, 23
A	WO 98 02793 A (ALLIED SIGNAL INC) 22 January 1998 (1998-01-22) abstract page 3, line 12 - line 22	2,12,20, 23

-/---

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2000	26/04/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lievens, K

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int(Jonal Application No
PCT/US 99/25761

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 689 565 A (SPELMAN JEFFREY F ET AL) 18 November 1997 (1997-11-18) column 8, line 61 -column 10, line 9	2,12,20, 23

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/US 99/25761

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5757908 A	26-05-1998	US 5598470 A	28-01-1997
		CA 2145922 A,C	26-10-1995
		EP 0681233 A	08-11-1995
		JP 7306780 A	21-11-1995
		KR 188505 B	01-06-1999
EP 0665486 A	02-08-1995	US 5509074 A	16-04-1996
		CA 2137065 A	28-07-1995
		JP 7239828 A	12-09-1995
WO 9802793 A	22-01-1998	EP 0910821 A	28-04-1999
US 5689565 A	18-11-1997	NONE	